**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF DELAWARE**

| | | |
|---|---|---|
| JORDAN STEIN, individually and on behalf of others similarly situated, | ) | |
| Plaintiffs, | ) | Case No. |
| v. | ) | **JURY TRIAL DEMANDED** |
| CLARIFAI, INC., | ) | |
| Defendant. | ) | |

## CLASS ACTION COMPLAINT

Plaintiff, Jordan Stein, individually and on behalf of all others similarly situated, brings this class action complaint against Defendant Clarifai, Inc. ("Clarifai" or "Defendant") for its violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA") and alleges as follows:

## NATURE OF THE ACTION

1. The past two decades have seen an exponential growth in technologies capable of verifying a person's identity based on his or her "biometric identifiers"—*i.e.* unique physical features such as fingerprints, retina scans, and scans of hand or facial geometry. *See* 740 ILCS 14/10.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers" such as social security numbers, which can be changed if compromised. 740 ILCS 14/5(c). "Biometrics . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. Recognizing the need to protect citizens from these risks, Illinois enacted BIPA,

which prohibits private entities like Clarifai from obtaining and/or possessing an individual's biometrics unless they first: (1) inform that person in writing that biometric identifiers or information will be collected or stored; (2) provide that person with written notice of the specific purpose and length of term for which such biometric identifiers and/or information is being collected, stored, and used; (3) receive a signed written release from the person authorizing the collection of his or her biometric identifiers and/or information; and (4) develop and comply with a publicly-available retention schedule and guidelines for permanently destroying the biometric identifiers and/or information within certain timeframes. *See* 740 ILCS 14/15(a)-(b).

4. In direct violation of these requirements, Clarifai—an industry leader in artificial intelligence and machine learning—collected, captured, obtained, used, and profited from the facial geometry of tens (if not hundreds) of thousands of unwitting Illinois citizens. With the assistance of its Chicago-based investors, Clarifai secretly accessed the subject profile photographs that people had uploaded to OKCupid, one of the world's largest dating websites. After obtaining these images, Clarifai scanned the facial geometry of each individual depicted therein to create unique "face templates," which it used to develop and train its facial recognition technology.

5. BIPA also makes it unlawful for private entities such as Clarifai to profit from a person's biometric identifiers or information. *See* 740 ILCS 14/15(c). Nevertheless, Clarifai continuously and systematically marketed and sold its facial recognition technology derived from the illegally-obtained biometric identifiers and/or information to customers throughout the United States—including in Illinois.

6. Accordingly, Plaintiff, on behalf of herself and all other similarly-situated individuals, brings this action to prevent Clarifai from further violating the privacy rights of those Illinois residents affected by its biometric-harvesting scheme, and to recover statutory damages

for Clarifai's unlawful collection, storage, use, and commercial exploitation of those individuals' biometric identifiers and/or information.

## PARTIES

7. Defendant Clarifai is a private, for-profit corporation organized under Delaware law and headquartered in New York, New York.

8. Founded in 2013, Clarifai is an artificial intelligence company that offers a variety of autonomous image-recognition services including but not limited to facial recognition technology. Clarifai markets and sells this technology throughout the United States, including in Illinois.

9. Plaintiff Jordan Stein is, and has been at all relevant times, a resident and citizen of Illinois. Clarifai collected, obtained, stored, used, possessed, and profited from Plaintiff's biometric identifiers and/or information—specifically, scans of her unique facial geometry.

## JURISDICTION AND VENUE

10. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) because this is a class action in which at least one member of the proposed class of plaintiffs is a citizen of a State different from Clarifai within the meaning of 28 U.S.C. § 1332(d), and the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs. The Court has supplemental jurisdiction over the state law claim pursuant to 28 U.S.C. § 1367.

11. This Court has personal jurisdiction over Clarifai because it is incorporated in the State of Delaware.

12. Venue is proper under 28 U.S.C. § 1391(b)(1) because Clarifai resides in this District.

## FACTUAL BACKGROUND

### I. Illinois' Biometric Information Privacy Act

13. Biometrics are unlike other identifiers because they are a permanent, biologically-unique identifier associated with the individual. Because one cannot simply change her fingerprints or facial geometry, the collection, use, and storage of biometric identifiers and biometric information creates a heightened risk of identity theft. *See* 740 ILCS 14/5(c).

14. In the 2000's, major national corporations started using Chicago and other locations in Illinois to test new applications of biometric-facilitated transactions. *See* 740 ILCS 14/5(b).

15. In late 2007, a biometrics company called Pay by Touch—which provided major retailers throughout the State of Illinois with biometric scanners to facilitate consumer transactions—filed for bankruptcy. That bankruptcy was alarming to the Illinois legislature because suddenly there was a serious risk that citizens' biometric records—which can be linked to people's sensitive financial and personal data—could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections. The bankruptcy also highlighted that many persons who used the biometric scanners were unaware that the scanners were transmitting their data to the now-bankrupt company, and that their biometric identifiers and information could then be sold to unknown third-parties.

16. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. Illinois House Transcript, 2008 Reg. Sess. No. 276, p.249 (May 30, 2008); *see also* 740 ILCS 14/5(g).

17. BIPA makes it unlawful for a company to collect, capture, purchase, receive through trade, or otherwise obtain a person's biometric identifier or information unless the company first:

a) informs the subject in writing that a biometric identifier or information is being

collected or stored;

b) informs the subject in writing of the specific purpose and length of term for which a biometric identifier or information is being collected, stored, and used; and

c) receives a written release executed by the subject of the biometric identifier or information.

740 ILCS 14/15(b).

18. BIPA defines a "written release" as "informed written consent." 740 ILCS 14/10.

19. BIPA also requires companies to develop and comply with a written policy—made available to the public—establishing a retention schedule and guidelines for permanently destroying biometric identifiers and information when the initial purpose for collecting such identifiers or information has been satisfied, or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

20. BIPA further prohibits a private entity in possession of a biometric identifier or information from selling, leasing, trading, or otherwise profiting from it. 740 ILCS 14/15(c)-(d).

## II. The Growing Use, and Dangers, of Facial Recognition Technology

21. One of the most prevalent uses of biometric identifiers and biometric information is in facial recognition, a powerful form of artificial intelligence that matches a person's image to a database of stored photos.

22. Facial recognition technology is based on algorithms that learn how to recognize human faces and the hundreds of ways in which each face is unique.

23. These algorithms create a unique "face template" of a person's facial geometry by scanning, identifying and taking measurements related to various facial landmarks, such as the location of the mouth, chin, nose, ears, eyes and eyebrows.

24. To automatically extract face templates from new images, a facial recognition

algorithm must be "trained" to identify and measure the relevant facial landmarks.

25. This is typically accomplished by the algorithm evaluating "triplet" sets of photographs—*i.e.* two images of the same person (known as the "anchor" and "positive sample"), and one image of a completely different person (known as the "negative sample").

26. The algorithm reviews the measurements collected from each image, and then adjusts itself so that the measurements collected from the anchor sample are more like those collected from the positive sample, and less like from those collected from the negative sample.

27. After repeating this process millions of times with images of thousands of different people, the algorithm learns to reliably scan for and collect a face template of any given face.

28. The use of facial recognition technology in the commercial context presents numerous privacy concerns. During a 2012 hearing before the United States Senate Subcommittee on Privacy, Technology, and the Law, U.S. Senator Al Franken stated that "there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop and carefully consider the way we use [it], it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[1] Senator Franken noted, for example, that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[2]

29. Senator Franken's concerns were well-founded, as law enforcement agencies have already used facial recognition technology to conduct warrantless surveillance at political

[1] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012), *available at* https://www.judiciary.senate.gov/download/statement-of-franken-pdf (last visited Feb. 7, 2020).

[2] *Id.*; *see also* Antonia Diener, *Can You See Me Now? Facial Surveillance Is a Civil Liberties Issue*, Harv. C.R.-C.L. L. Rev., Nov. 13, 2019, *available at* https://harvardcrcl.org/can-you-see-me-now-facial-surveillance-is-a-civil-liberties-issue/.

protests.[3]

30. Equally problematic, studies confirm facial recognition technology can be highly inaccurate with respect to identifying women and people of color. A recent federal study found that African Americans and Asians are roughly 100 times more likely to be misidentified than Caucasian men, and women are misidentified at a far higher rate than men.[4]

## III. Clarifai Secretly and Illegally Harvests the Class Members' Biometric Identifiers

31. The process of training facial recognition algorithms requires vast quantities of images from a diverse array of faces.

32. To satisfy the ever-growing demand for myriad high-resolution images of faces, many companies have resorted to the controversial practice known as "face scraping," which entails scouring the internet for vast quantities of photos and extracting the subjects' unique facial geometry—all without the subjects' knowledge or consent.[5] Oftentimes, companies simply grab whatever images they can find "in the wild." This has been called the "dirty little secret" of artificial intelligence.

33. Clarifai pursued a similar strategy. As first revealed in a July 13, 2019 New York Times article, Clarifai built a massive "face database" (the "Database") using profile photographs

[3] *See* Terry Collins, *Facial Recognition: Do You Really Control How your Face is Being Used?*, USA Today, December 23, 2019, *available at* https://www.usatoday.com/story/tech/2019/11/19/police-technology-and-surveillance-politics-of-facial-recognition/4203720002/.

[4] *See* Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, Washington Post, December 18, 2019, *available at* https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[5] Ian Carlos Campbell, *Clearview AI hit with sweeping legal complaints over controversial face scraping in Europe*, The Verge, May 27, 2021, *available at* https://www.theverge.com/2021/5/27/22455446/clearview-ai-legal-privacy-complaint-privacy-international-facial-recognition-eu.

of users of OKCupid, a popular dating website.[6]

34. Clarifai surreptitiously gained access to those profile photographs through one of Clarifai's investors, a Chicago-based venture capital group launched by OKCupid's founders.

35. Clarifai created the Database to develop and train the algorithms used in its facial recognition technology. To that end, Clarifai created thousands of unique face templates by scanning, extracting, storing, and using the unique facial geometry of each face detected in the profile photographs.

36. Clarifai did not notify those Illinois residents whose photographs appeared in the Database about the collection and storage of their biometric identifiers or biometric information, nor did Clarifai obtain a signed written release from any of those individuals. *See* 740 ILCS 14/15(b)(1), (3).

37. Clarifai did not inform those individuals about the purpose and length of the term for which their biometric identifiers and biometric information would be collected, stored, and used. *See* 740 ILCS 14/15(b)(2).

38. Clarifai does not have a written, publicly-available policy establishing a retention schedule and guidelines for permanently destroying Plaintiff's and the Class members' biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

39. Clarify has not permanently destroyed Plaintiff's and the Class members' biometric identifiers and biometric information as required by BIPA. *See* 740 ILCS 14/15(a).

40. Clarifai did not notify Plaintiff or the Class members that Clarifai (or anyone else) had gained access to their OKCupid profile photographs.

---

[6] Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, New York Times, July 13, 2019, *available at* https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

41. Given the secretive nature of the scheme, Plaintiff and the Class members had no way of knowing Clarifai had gained access to their OKCupid profile photographs or collected, used and profited from their biometric identifiers and biometric information until those facts were first revealed in a July 13, 2019 New York Times article.

42. In the same article, Clarifai's CEO, Matt Zeiler, revealed that the company signed an agreement with a large social media company to use the social media company's users' images for training facial recognition algorithms. Zeiler did not, however, disclose the name of this social media company.

43. Thus, Clarifai's surreptitious harvesting of biometric identifiers and biometric information is ongoing.

44. Clarifai sells its facial recognition technology to customers throughout the United States, including in Illinois.

45. Zeiler has publicly stated that Clarifai will sell its facial recognition technology to foreign governments.

46. In or around July 2017, Clarifai began working on a drone surveillance program for the Department of Defense known as "Project Maven," a controversial project designed to create autonomous weapons.

47. In January 2019, then-Clarifai-employee Liz O'Sullivan posted an open letter to CEO Matt Zeiler (the "Open Letter") on the company message board.

48. Liz O'Sullivan managed Clarifai's face Database and was originally tapped to serve as an ethics advisor of Clarifai.

49. The Open Letter to Matt Zeiler voiced Ms. Sullivan's and other Clarifai employees' concerns and stated, *inter alia*, the following:

a) "Google and Amazon employees' open letters have described some of the more obvious applications of CFR [*i.e.* Computerized Facial Recognition] that are terrifying (mass surveillance, social credit scoring, political oppression/registration), but there is a fourth elephant in the room that few are addressing: autonomous weapons."

b) "We in the industry know that all technology can be compromised. Hackers hack. Bias is unavoidable."

c) "We very nearly went live with a version of CFR that had 10% more errors when predicting on people with dark skin. If this technology had been sold to a government for security purposes, it would certainly have a negative effect on all the dark-skinned people who would be disproportionately mistaken for criminals."

d) "[T]he last questions we have relate [to] our philosophy on data collection. Because the way we treat consumer data is an important part of our ethical framework. It demonstrates how far we are willing to go in the interest of profit, at the expense of privacy and consent. And just this month, we've been asked to download data from cameras whose owners haven't given consent at all . . . and a few other sources that may walk a legal line but are sketchy at best."

e) "All of these things combined with the change in plan regarding our board ethics committee lead us to ask the following questions: . . .

- Will Clarifai vet every military contract to ensure that our work does not get used in the creation of autonomous weapons? . . .
- Will Clarifai promise not to sell CFR (or any similar technology that has the potential to be used for oppression) to any totalitarian or otherwise oppressive government for any purpose ever? . . .
- Will Clarifai promise to evaluate every algorithm we build for racial/age/gender/disability bias as part of our process, and not just as an ad hoc afterthought? . . .
- Will Clarifai promise never to use illegally obtained or otherwise ethically dubious data?"

50. Approximately one week later, Clarifai CEO Matt Zeiler called a company-wide meeting and announced that Clarifai's facial recognition technology would be used for autonomous weapons. Zeiler explained that, while Clarifai would not be building missiles, its technology is going to be useful for them and will make its way into autonomous weapons through Clarifai's partnerships.

## IV. Facts Pertaining to Plaintiff Stein

51. In 2013, Plaintiff created a user profile with OKCupid.

52. At that time, Plaintiff uploaded approximately five (5) digital photographs of herself to OKCupid.

53. Plaintiff created, uploaded, and managed those photographs from computers and mobile devices located in Illinois.

54. At all relevant times, Plaintiff's OKCupid user profile identified her as a Chicago resident and provided a method for contacting her directly through OKCupid's message system.

55. Plaintiff maintained an OKCupid user profile from 2013 through present day.

56. Plaintiff maintained an OKCupid user profile when Clarifai obtained the profile photographs it used to create the Database. Thus, Plaintiff's profile photographs are contained in the Database.

57. As with the other photographs in the Database, Clarifai captured biometric identifiers and biometric information from Plaintiff's profile photographs by identifying, scanning and measuring her facial landmarks and using that data to create a unique template of Plaintiff's facial geometry.

58. Clarifai stored and used Plaintiff's face template (scans of face geometry) in the same manner as the other templates collected from photographs in the Database—to train and develop Clarifai's facial recognition technology that Clarifai sells to customers throughout the United States and abroad.

59. At no time did Clarifai inform Plaintiff, in writing or otherwise, about the collection, receipt, storage, or use of her biometric identifiers or biometric information.

60. At no time did Clarifai notify Plaintiff, in writing or otherwise, about the purpose

and length of time for which her biometric identifiers and biometric information were being collected, stored, and used.

61. At no time did Plaintiff provide Clarifai with an executed written release authorizing the collection, receipt, storage, and/or use of her biometric identifiers and biometric information.

62. Plaintiff has never given Clarifai informed written consent to collect, capture, receive, store or use her facial geometric data.

63. Plaintiff would not have given Clarifai informed written consent to collect or use her biometric identifiers or biometric information for the purpose of training facial recognition software for Clarifai's own profit.

64. Plaintiff was not informed of any biometric data retention policy of Clarifai, nor has she ever been informed as to whether and when Clarifai will ever permanently delete her facial geometric data.

## V. Plaintiff's and the Class Members' Injuries

65. As a result of Clarifai's unlawful conduct, Plaintiff and the other members of the Class have already sustained information and privacy injuries in Illinois and face additional imminent, impending injuries.

66. Clarifai chose to use and profit from biometric identifiers and information obtained from photographs that were: (1) created in Illinois; (2) uploaded from Illinois; (3) managed via Illinois-based user accounts from computers and mobile devices in Illinois; and (4) stored on servers located in Chicago, Illinois. In so doing, Clarifai exposed Illinois residents and citizens to ongoing privacy risks in Illinois, knowing its conduct would injure those residents and citizens in Illinois.

67. Further, Clarifai knew (or had reason to know) obtaining and profiting from Illinois residents' and citizens' biometric identifiers and biometric information in violation of BIPA would deprive those residents and citizens of their statutorily-protected information and privacy rights, neutralize their respective abilities to control access to their biometric identifiers and biometric information via their Illinois-based devices, and expose them to potential surveillance and other privacy harms. As such, Illinois has a direct interest in regulating the unlawful conduct alleged herein in order to protect the rights of its citizens and residents.

68. As the Illinois Legislature has found and the Illinois Supreme Court has confirmed, the harm to Plaintiff and the Class from the BIPA violations alleged herein has already occurred.

69. Moreover, as businesses vie to develop ever more advanced facial recognition technology, the race for the data required to fuel those developments threatens the privacy of individuals everywhere, including Plaintiff and the Class. Given the risks of unwanted data collection and disclosure, public policy in Illinois expressly provides its citizens with the right to control the fate of their unique biometric identifiers and information. Clarifai's actions—including, but not limited to, its failure to provide the necessary disclosures and obtain the requisite consent—deprived Plaintiff and the Class of this right.

70. Due to Clarifai's illegal actions, Plaintiff's and the Class's biometric identifiers and/or information is no longer under their control and are available to a potentially unlimited range of unknown individuals, exposing Plaintiff and the Class to the imminent and certainly impending injuries of identity theft, fraud, stalking, surveillance, and other invasions of privacy.[7]

[7] Samir Jeraj, *With facial recognition technology, how safe is your data?*, The New Statesman, March 2, 2020, *available at* https://www.newstatesman.com/spotlight/cyber/2020/03/facial-recognition-technology-how-safe-your-data.

71. Hackers have infiltrated Clarifai's computer systems on at least one occasion since Clarifai obtained the OK Cupid users' photographs and created the Database.[8]

72. And there is already an illegal market for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data—including fingerprints, iris scans, and facial photographs—of over one billion citizens of India.[9] In January 2018, an Indian newspaper reported that, as part of a sting, it only took the newspaper about 10 minutes and less than $7.00 to purchase the data housed in Aadhaar, and for a mere $4.00 more, it also purchased the software needed to misuse that data for fraud.[10]

73. By collecting Plaintiff's and the Class members' unique biometric identifiers and biometric information without their consent, written or otherwise, Clarifai invaded their statutorily protected right to privacy in their biometrics.

74. Clarifai's acts and omissions denied Plaintiff and the Class members the opportunity to consider whether the terms of Clarifai's collection, storage and use of, and profiting from, their biometric identifiers and biometric information were acceptable given the attendant risks, and denied them the ability to use the undisclosed information in the way BIPA envisioned, all of which harmed their concrete interests that the legislature sought to protect by enacting BIPA.

---

[8] *See* Tom Simonite, *Startup Working on Contentious Pentagon AI Project Was Hacked*, Wired (June 12, 2018, 9:07 p.m.), https://www.wired.com/story/startup-working-on-contentious-pentagon-ai-project-was-hacked/.

[9] Vidhi Doshi, *A security breach in India has left a billion people at risk of identity theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/.

[10] Rachna Khaira, *Rs 500, 10 minutes, and you have access to billion Aadhaar details*, The Tribune (Jan. 4, 2018), *available at* https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361.

75. Clarifai's failure to delete Plaintiff's and the Class members' biometric identifiers and biometric information resulted in Clarifai's unlawful retention of their biometric data, thereby inflicting a concrete and particularized privacy injury separate and distinct from Clarifai's unlawful collection of their biometric identifiers and biometric information.

76. By profiting from Plaintiff's and the Class members' biometric identifiers and biometric information, Clarifai deprived them of the opportunity to profit from their biometric identifiers and biometric information, thereby inflicting a concrete and particularized injury separate and distinct from Clarifai's unlawful collection and retention of their biometric identifiers and biometric information.

77. By profiting from Plaintiff's and the Class's biometric identifiers and biometric information, Clarifai also exacerbated the harm resulting from the privacy violation that occurred when it unlawfully collected their biometric identifiers and biometric information in the first place.

78. As a result of Clarifai's misconduct, Plaintiff and the Class have no recourse for the fact that their biologically-unique information has been compromised, and are likely to withdraw from biometric-facilitated transactions and other facially-mediated electronic participation.

## CLASS ALLEGATIONS

79. Plaintiff brings this action on behalf of herself and a class of similarly-situated individuals defined, subject to amendment, as follows:

> All Illinois residents who had their biometric identifiers, biometric information, or scans of their face geometry collected, captured, purchased, received through trade, or otherwise obtained, and/or stored, and/or used, and/or profited from, by Clarifai at any time from February 13, 2015 through trial.

80. Plaintiff represents and is a member of the Class. The following people are

excluded from the Class: (1) any judge presiding over the action and their families and staff; (2) Defendant and its owners, officers, directors, parents, subsidiaries, successors, predecessors; and (3) Plaintiff's and Defendant's counsel and their staffs.

81. Plaintiff and the other members of the Class have been harmed by Clarifai's acts and omissions.

82. Certification of Plaintiff's claim for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

83. **Numerosity.** The members of the Class are so numerous that individual joinder of all Class members is impracticable. Clarifai unlawfully harvested biometric identifiers from more than 60,000 OKCupid users residing in Illinois. While the exact number of Class member is currently unknown to Plaintiff, this information can be ascertained from Clarifai's books and records, as well as OKCupid's records. Class members can be notified about the pendency of this action through recognized, Court-approved methods of notice dissemination, such as U.S. Mail, electronic mail, internet postings, and/or published notice.

84. **Commonality and Predominance.** This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a) whether Clarifai collected, captured, or otherwise obtained the Class members' biometric identifiers or biometric information;

b) whether Clarifai possessed the Class members' biometric information;

c) whether Clarifai informed the Class members in writing that their biometric identifiers and biometric information are being collected or stored;

d) whether Clarifai informed Class members in writing of the specific purposes and length of term for which their biometric identifiers and biometric information are being collected, stored, and used;

e) whether Clarifai received a signed written release (as defined in 740 ILCS 14/10) to collect, capture, use, and store each Class member's biometric identifiers and biometric information;

f) whether Clarifai disclosed or re-disclosed the Class members' biometric identifiers or biometric information to any third-party;

g) whether Clarifai sold, leased, traded, or otherwise profited from the Class members' biometric identifiers or biometric information;

h) whether Clarifai maintained a publicly-available written policy establishing a retention schedule and guidelines for the destruction of biometric identifiers and information at the time it collected the Class members' biometric identifiers and biometric information;

i) whether Clarifai complied with any such written policy;

j) whether Clarifai permanently destroyed the Class members' biometric identifiers and biometric information;

k) whether Clarifai violated BIPA; and

l) whether Clarifai's BIPA violations were negligent, reckless, or intentional.

85. **Typicality.** Plaintiff's claims are typical of the claims of the Class she seeks to represent, as Plaintiff and all members of the proposed Class have suffered similar injuries as a result of the same practices alleged herein.

86. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex and class action litigation. Plaintiff and her counsel are committed to vigorously prosecuting this class action. Neither Plaintiff nor her counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiff has raised viable statutory claims of the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiff may seek leave of this Court to amend this Class Action Complaint to include

additional Class representatives to represent the Class, additional claims as may be appropriate, or to amend the Class definition to address any steps that Clarifai took.

87. **Superiority.** A class action is appropriate to resolve the claims at issue because: (i) the prosecution of separate actions by the members of the Class would wastefully burden the judicial system with the need to resolve over and over the common factual and legal questions this case presents; (ii) requiring members of the Class to prosecute their own individual lawsuits would work an injustice, as it would prevent Class members who are unaware they have a claim, or lack the time, ability, or wherewithal to bring their own lawsuit and find a lawyer willing to take their case, to obtain relief; (iii) requiring individual Class member lawsuits would create a risk of adjudications with respect to individual members of the Class that would, as a practical matter, be dispositive of the interests of the other members not parties to the adjudications, or substantially impair or impede their ability to protect their interests, or create conflicting and incompatible standards of conduct; and (iv) proceeding on a class basis will not create any significant difficulty in the management of this litigation, as the Class members will be easily identified from the business records of Clarifai and third parties (*e.g.* OkCupid), and the Class members' claims can be proven using common evidence. Thus, there will be no difficulty maintaining this case as a class action.

## COUNT I
## Violation of 740 ILCS 14/15(b)
## (On Behalf of Plaintiff and the Class)

88. Plaintiff incorporates the above allegations as if fully set forth herein.

89. BIPA requires private entities such as Clarifai to obtain informed written consent from individuals before acquiring their biometric data. Specifically, BIPA makes it unlawful for any "private entity" to "collect, capture, purchase, receive through trade, or otherwise obtain a

person's . . . biometric identifier or biometric information, unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; **and** (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

90. Clarifai is a corporation, and thus constitutes a "private entity" under BIPA. *See* 740 ILCS 14/10.

91. Plaintiff and the Class members are individuals whose "biometric identifiers" and "biometric information," as defined by the BIPA—including, without limitation, scans of their facial geometry—were collected, captured, purchased, received through trade or otherwise obtained, stored, and used by Clarifai.

92. Clarifai violated BIPA by failing to inform Plaintiff and the Class, in writing, about the collection and storage of their biometric identifiers and biometric information before it occurred. *See* 740 ILCS 14/15(b)(1).

93. Clarifai violated BIPA by failing to inform Plaintiff and the Class, in writing before the fact, of the specific purpose and length of term for which their biometric identifiers and biometric information were being "collected, stored, and used." *See* 740 ILCS 14/15(b)(2).

94. Clarifai violated BIPA by collecting, capturing, purchasing, receiving through trade, and otherwise obtaining Plaintiff's and the Class members' biometric identifiers and biometric information without first obtaining a signed written release from each of them. *See* 740 ILCS 14/15(b)(3).

95. In so doing, Clarifai deprived Plaintiff and the Class of their statutory right to

maintain the privacy of their biometric identifiers and biometric information.

96. Clarifai carried out a deliberate scheme to secretly harvest biometric identifiers and biometric information from millions of individuals, including Plaintiff and the Class members, without their knowledge or consent.

97. Clarifai's conduct intentionally or recklessly violated BIPA with respect to Plaintiff and the Class members.

98. In the alternative, Clarifai's conduct negligently violated BIPA with respect to Plaintiff and the Class members.

99. Accordingly, Plaintiff, on behalf of herself and the Class, seeks: (1) declaratory relief; (2) statutory damages of $5,000 for each intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); (3) injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Clarifai to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information, as described herein; and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

## COUNT II
**Violation of 740 ILCS 14/15(c)**
**(On Behalf of Plaintiff and the Class)**

100. Plaintiff restates and re-alleges all paragraphs of this Complaint as though fully set forth herein.

101. BIPA makes it unlawful for private entities in possession of biometric identifiers or biometric information to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

102. Clarifai is a corporation, and thus constitutes a "private entity" under BIPA. *See* 740 ILCS 14/10.

103. Clarifai is in possession of Plaintiff's and the Class members' biometric identifiers and biometric information.

104. Clarifai used Plaintiff's and the Class members' biometric identifiers and biometric information to train and develop its facial recognition technology, which Clarifai sells to customers throughout the United States.

105. In so doing, Clarifai violated BIPA by profiting from Plaintiff's and the Class members' biometric identifiers and biometric information. *See* 740 ILCS 14/15(c).

106. By profiting from their biometric identifiers and biometric information, Clarifai deprived Plaintiff and the Class members of the opportunity to profit from their biometric identifiers and biometric information.

107. Clarifai carried out a premeditated plan to commercially exploit the biometric identifiers and biometric information that Clarifai illegally harvested from Plaintiff and the Class members.

108. Clarifai's conduct intentionally or recklessly violated BIPA with respect to Plaintiff and the Class members.

109. In the alternative, Clarifai's conduct negligently violated BIPA with respect to Plaintiff and the Class members.

110. Accordingly, Plaintiff, on behalf of herself and the Class, seeks: (1) declaratory relief; (2) statutory damages of $5,000 for each intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); (3) injunctive and other equitable relief as is

necessary to protect the interests of Plaintiff and the Class by preventing Clarifai from continuing to commercially exploit their biometric identifiers and biometric information; and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

**COUNT III**
**Violation of 740 ILCS 14/15(a)**
**(On Behalf of Plaintiff and the Class)**

111. Plaintiff restates and re-alleges all paragraphs of this Complaint as though fully set forth herein.

112. BIPA requires private entities in possession of biometric data to establish and maintain a satisfactory biometric data retention—and, importantly, deletion—policy. Specifically, those entities must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent destruction of biometric data (at most three years after the entity's last interaction with the individual); and (ii) adhere to that retention schedule and actually delete the biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

113. Clarifai failed to comply with either of these BIPA mandates.

114. Clarifai is a corporation, and thus constitutes a "private entity" under BIPA. *See* 740 ILCS 14/10.

115. Clarifai is in possession of Plaintiff's and the Class members' biometric identifiers and biometric information.

116. In violation of BIPA, Clarifai did not maintain the statutorily-mandated retention schedule and destruction guidelines at the time it collected Plaintiff's and the Class member's biometric identifiers and biometric information. *See* 740 ILCS 14/15(a).

117. In violation of BIPA, Clarifai did not permanently destroy Plaintiff's and the Class members' biometric identifiers and biometric information as required. *See* 740 ILCS 14/15(a).

118. By failing to destroy Plaintiff's and the Class members' biometric identifiers and biometric information, Clarifai unlawful retained their biometric data.

119. Clarifai's conduct intentionally or recklessly violated BIPA with respect to Plaintiff and the Class members.

120. In the alternative, Clarifai's conduct negligently violated BIPA with respect to Plaintiff and the Class members.

121. Accordingly, Plaintiff, on behalf of herself and the Class, seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Clarifai to immediately and permanently destroy their biometric identifiers and biometric information, and to comply with BIPA's requirements that private entities maintain and comply with publicly-available guidelines for permanently destroying biometric identifiers and biometric information; (3) statutory damages of $5,000 for each intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorney's fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

## COUNT IV
## Unjust Enrichment
## (On Behalf of Plaintiff and the Class)

122. Plaintiff restates and re-alleges all paragraphs of this Complaint as though fully set forth herein.

123. Clarifai obtained a monetary benefit from Plaintiff and the Class members, to their detriment, by profiting from the covert collection and use of their biometric identifiers and biometric information.

124. Clarifai's profiting from Plaintiff's and the Class members' biometric identifiers

and biometric information deprived Plaintiff and the Class members of the opportunity to profit from their biometric identifiers and biometric information.

125. Plaintiff and the Class members did not authorize Clarifai to collect, capture, receive, otherwise obtain, use, store, or profit from their biometric identifiers and biometric information.

126. Clarifai appreciated, accepted, and retained the benefits bestowed upon it under inequitable and unjust circumstances arising from its conduct toward Plaintiff and the Class as described herein.

127. In particular, Clarifai secretly obtained Plaintiff's and the Class members' profile photographs from a third-party for the sole purpose of harvesting their biometric identifiers and biometric information, without permission and in violation of Illinois law.

128. Clarifai used and profited from Plaintiff's and the Class member's biometric identifiers and biometric information without providing any compensation for the commercial benefits it received.

129. Under the principles of equity and good conscience, it would be unjust and unfair for Clarifai to be permitted to retain any of the benefits obtained from its unlawful collection and use of Plaintiff's and the Class members' biometric identifiers and biometric information.

130. Clarifai should be compelled to disgorge into a common fund or constructive trust all proceeds it unjustly received from the collection and use of Plaintiff's and the Class members' biometric identifiers and biometric information.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff Jordan Stein, on behalf of herself and the Class, respectfully requests that the Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above (or on behalf of any other class the Court deems appropriate);

B. Appointing Plaintiff as representative of the Class, and her undersigned attorneys as class counsel;

C. Declaring that Clarifai's acts and omissions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq*.;

D. Awarding statutory damages of $5,000 for each and every intentional or reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or alternatively, statutory damages of $1,000 for each and every negligent violation pursuant to 740 ILCS 14/20(1) if the Court finds that Clarifai's violations were negligent;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including, *inter alia*, requiring Clarifai to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information, to cease its unlawful practice of profiting from Plaintiff's and the Class's biometric identifiers and biometric information, and to permanently destroy Plaintiff's and the Class members' biometric identifiers and biometric information;

F. Requiring Clarifai to disgorge all profits it received from the collection and use of Plaintiff's and the Class members' biometric identifiers into a common fund or constructive trust;

G. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3);

H. Awarding Plaintiff and the Class members pre- and post-judgment interest, to the extent allowable; and

I. Awarding such other and further relief as equity and justice may require.

**JURY DEMAND**

Plaintiff, individually and on behalf of all others similarly situated, hereby demands trial by jury on all issues so triable.

Dated: March 10, 2022

COOCH and TAYLOR, P.A.

By: /s/ *Carmella P. Keener*

Carmella P. Keener (Del. No. 2810)
The Nemours Building
1007 N. Orange Street, Suite 1120
Wilmington, DE 19899-1680
302-984-3816
ckeener@coochtaylor.com

***Attorneys for Plaintiff and the Putative Class***

OF COUNSEL:

Keith J. Keogh
Theodore H. Kuyper
Gregg M. Barbakoff
KEOGH LAW, LTD.
55 W. Monroe St., Suite 3390
Chicago, Illinois 60603
(312) 726-1092
(312) 726-1093 (fax)
keith@keoghlaw.com
tkuyper@keoghlaw.com
gbarbakoff@keoghlaw.com